Encyclopedia of Mathematics and Its Applications 157

SOLVING POLYNOMIAL EQUATION SYSTEMS III

Algebraic Solving

Teo Mora

CAMBRIDGE

This third volume of four finishes the program begun in Volume I by describing all the most important techniques, mainly based on Gröbner bases, which allow one to manipulate the roots of an equation rather than just compute them.

The book begins with the "standard" solutions (Gianni–Kalkbrener Theorem, Stetter Algorithm, the Cardinal–Mourrain result) and then moves on to more innovative methods (Lazard triangular sets, Rouillier's Rational Univariate Representation, the TERA Kronecker package). The author also looks at classical results, such as Macaulay's matrix, and provides a historical survey of elimination, from Bézout to Cayley.

This comprehensive treatment in four volumes is a contribution to algorithmic commutative algebra that will be essential reading for algebraists and algebraic geometers.

Teo Mora is a Professor of Algebra in the Department of Mathematics at the University of Genoa.

Praise for Volumes I and II

"I took great pleasure in reading this book and, in my opinion, it should become the *livre de chevet* of people working in the part of computer algebra that deals with univariate polynomials." *Mathematical Reviews*

"I fell in love with this book at first sight; for it is not just extremely well organized, it is also written in a style that is a joy to read... To sum up, this is a wonderful book, beautifully written and produced, that should be in every mathematical library." *SIGACT News*

"...a fabulous undergraduate introduction to modern algebra, simultaneously foundational and computational. Highly recommended." *Choice*

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-0-521-81155-2
9 780521 811552

157

Mora

SOLVING POLYNOMIAL EQUATION SYSTEMS III

CAMBRIDGE

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Solving Polynomial Equation Systems

Volume III: Algebraic Solving

TEO MORA

University of Genoa

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521811552

First published 2015

A catalogue record for this publication is available from the British Library

ISBN – Volume I 978-0-521-81154-5 Hardback
ISBN – Volume II 978-0-521-81156-9 Hardback
ISBN – Volume III 978-0-521-81155-2 Hardback
ISBN – Volume IV 978-1-107-10963-6 Hardback

SOLVING POLYNOMIAL EQUATION SYSTEMS

Volume III: Algebraic Solving

This third volume of four finishes the program begun in Volume I by describing all the most important techniques, mainly based on Gröbner bases, which allow one to manipulate the roots of an equation rather than just compute them.

The book begins with the "standard" solutions (the Gianni–Kalkbrener Theorem, Stetter Algorithm, the Cardinal–Mourrain result) and then moves on to more innovative methods (Lazard triangular sets, Rouillier's Rational Univariate Representation, the TERA Kronecker package). The author also looks at classical results, such as Macaulay's matrix, and provides a historical survey of elimination, from Bézout to Cayley.

This comprehensive treatment in four volumes is a contribution to algorithmic commutative algebra that will be essential reading for algebraists and algebraic geometers.

Encyclopedia of Mathematics and Its Applications

This series is devoted to significant topics or themes that have wide application in mathematics or mathematical science and for which a detailed development of the abstract theory is less important than a thorough and concrete exploration of the implications and applications.

Books in the **Encyclopedia of Mathematics and Its Applications** cover their subjects comprehensively. Less important results may be summarized as exercises at the ends of chapters. For technicalities, readers can be referred to the bibliography, which is expected to be comprehensive. As a result, volumes are encyclopedic references or manageable guides to major subjects.

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing visit www.cambridge.org/mathematics.

109 J. M. Borwein and J. D. Vanderwerff *Convex Functions*
110 M.-J. Lai and L. L. Schumaker *Spline Functions on Triangulations*
111 R. T. Curtis *Symmetric Generation of Groups*
112 H. Salzmann *et al. The Classical Fields*
113 S. Peszat and J. Zabczyk *Stochastic Partial Differential Equations with Lévy Noise*
114 J. Beck *Combinatorial Games*
115 L. Barreira and Y. Pesin *Nonuniform Hyperbolicity*
116 D. Z. Arov and H. Dym *J-Contractive Matrix Valued Functions and Related Topics*
117 R. Glowinski, J.-L. Lions and J. He *Exact and Approximate Controllability for Distributed Parameter Systems*
118 A. A. Borovkov and K. A. Borovkov *Asymptotic Analysis of Random Walks*
119 M. Deza and M. Dutour Sikirić *Geometry of Chemical Graphs*
120 T. Nishiura *Absolute Measurable Spaces*
121 M. Prest *Purity, Spectra and Localisation*
122 S. Khrushchev *Orthogonal Polynomials and Continued Fractions*
123 H. Nagamochi and T. Ibaraki *Algorithmic Aspects of Graph Connectivity*
124 F. W. King *Hilbert Transforms I*
125 F. W. King *Hilbert Transforms II*
126 O. Calin and D.-C. Chang *Sub-Riemannian Geometry*
127 M. Grabisch *et al. Aggregation Functions*
128 L. W. Beineke and R. J. Wilson (eds.) with J. L. Gross and T. W. Tucker *Topics in Topological Graph Theory*
129 J. Berstel, D. Perrin and C. Reutenauer *Codes and Automata*
130 T. G. Faticoni *Modules over Endomorphism Rings*
131 H. Morimoto *Stochastic Control and Mathematical Modeling*
132 G. Schmidt *Relational Mathematics*
133 P. Kornerup and D. W. Matula *Finite Precision Number Systems and Arithmetic*
134 Y. Crama and P. L. Hammer (eds.) *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*
135 V. Berthé and M. Rigo (eds.) *Combinatorics, Automata and Number Theory*
136 A. Kristály, V. D. Rădulescu and C. Varga *Variational Principles in Mathematical Physics, Geometry, and Economics*
137 J. Berstel and C. Reutenauer *Noncommutative Rational Series with Applications*
138 B. Courcelle and J. Engelfriet *Graph Structure and Monadic Second-Order Logic*
139 M. Fiedler *Matrices and Graphs in Geometry*
140 N. Vakil *Real Analysis through Modern Infinitesimals*
141 R. B. Paris *Hadamard Expansions and Hyperasymptotic Evaluation*
142 Y. Crama and P. L. Hammer *Boolean Functions*
143 A. Arapostathis, V. S. Borkar and M. K. Ghosh *Ergodic Control of Diffusion Processes*
144 N. Caspard, B. Leclerc and B. Monjardet *Finite Ordered Sets*
145 D. Z. Arov and H. Dym *Bitangential Direct and Inverse Problems for Systems of Integral and Differential Equations*
146 G. Dassios *Ellipsoidal Harmonics*
147 L. W. Beineke and R. J. Wilson (eds.) with O. R. Oellermann *Topics in Structural Graph Theory*
148 L. Berlyand, A. G. Kolpakov and A. Novikov *Introduction to the Network Approximation Method for Materials Modeling*
149 M. Baake and U. Grimm *Aperiodic Order I: A Mathematical Invitation*
150 J. Borwein *et al. Lattice Sums Then and Now*
151 R. Schneider *Convex Bodies: The Brunn–Minkowski Theory (Second Edition)*
152 G. Da Prato and J. Zabczyk *Stochastic Equations in Infinite Dimensions (Second Edition)*
153 D. Hofmann, G. J. Seal and W. Tholen (eds.) *Monoidal Topology*
154 M. Cabrera García and Á. Rodríguez Palacios *Non-Associative Normed Algebras I: The Vidav–Palmer and Gelfand–Naimark Theorems*
155 C. F. Dunkl and Y. Xu *Orthogonal Polynomials of Several Variables (Second Edition)*
156 L. W. Beineke and R. J. Wilson (eds.) with B. Toft *Topics in Chromatic Graph Theory*
157 T. Mora *Solving Polynomial Equation Systems III: Algebraic Solving*
158 T. Mora *Solving Polynomial Equation Systems IV: Buchberger Theory and Beyond*

Joachim of Fiore's *Age of the Holy Spirit* offers a Hegelian synthesis between the Old and New Testament.

A. Buendia, *The Long March of the Red Brigades through Conquest, War, Famine and Death*

God is my witness that I would sooner free your mind from mistakes than see me released from prison.

Martinek Húska Loquis

The computational effort required to implement this approach turned out to be orders of magnitude less than the effort which would be required by the direct techniques of decoding by exhaustive search. Using new techniques which are introduced in this book, it is now possible to build algebraic decoders which are orders of magnitude simpler than any that have previously been considered.

There is frequently a conflict between proofs which some people consider conceptually "simple" and proofs which lead to simple instrumentation. In this book I have attempted to provide the proofs which lead to the simplest implementations.

E.R. Berlekamp, *Algebraic Coding Theory*

Solomon Gandz in the final section of his introduction to the Mensuration of al-Khwarizmi wrote: "Euclid and his geometry [...] is entirely ignored by him when he writes on geometry. On the contrary, in the preface to his *Algebra*, Algorithm distinctly emphasizes his purpose of writing a popular treatise that, in contradiction to Greek theoretical mathematics, will serve the practical ends and needs of the people in their affairs of inheritance and legacies, in their law suits, in trade and commerces, in the surveying of lands and in the digging of canals. Hence, Algorithm appears to us not as a pupil of the Greeks but, quite to the contary, as the antagonist of [...] the Greek school, as the representative of the native popular science. At the Academy of Bagdad Algorithm represented rather the reaction against the introduction of Greek mathematics. His *Algebra* impresses us as a protest rather against the Euclid translation and against the whole trend of the reception of the Greek science."

Is it too much to read this quotation as a parable, interpreting Greeks as French and Euclid as Bourbaki?

R.F. Ree, *The Foundational Crisis, a Crisis of Computability?*

Preface

La gloria di colui che tutto move
per l'universo penetra, e risplende
in una parte piú e meno altrove.

My HOPE that this *SPES* series reaches completion has supported me over many years. These years have been devoted both to fixing the details of the operative scheme based on Spear's Theorem, which allows one to set a Buchberger Theory over each effective associative ring and of which I have been aware since my 1988 preprint "Seven variations on standard bases" and to satisfy my *horror vacui* by including all the relevant results of which I have been aware.

My *horror vacui* had the negative aspect of making the planned third book grow too much, forcing me to split it into two separate volumes. As a consequence the structure I planned 12 years ago and which anticipated a Hegelian (or Dante-like) trilogy, whose central focus was the Gröbnerian technology discussed in Volume II, was quite deformed and the result appears as a (Wagner-like?) tetralogy.

This volume contains Part six, *Algebraic Solving*, and is where I complete the task set out in Part one by discussing all the recent approaches. These are mainly based on the results discussed in Volume II, which allow one to effectively manipulate the roots of a polynomial equation system, thus fulfilling the aim of "solving" as set out in Volume I according to the Kronecker–Duval Philosophy: Trinks' Algorithm, the Gianni–Kalkbrener Theorem, the Stetter Algorithm, Dixon's resultant, the Cardinal–Mourrain Algorithm, Lazard's Solver, Rouillier's Rational Univariate Representation, the TERA Kronecker package.

Macaulay's Matrix and u-resultant, a historical tour of elimination from Bézout to Dixon, who was the last student of Cayley, the Lagrange resolvent and the investigation of it performed by Valibuze and Arnaudies are also covered.

Setting

1. Let k be an infinite, perfect field, where, if $p := \text{char}(k) \neq 0$, it is possible to extract pth roots, and let k be the algebraic closure of k and $\Omega(k)$ the universal field over k.

Let us fix an integer value n and consider the polynomial ring

$$\mathcal{P} := k[X_1, \ldots, X_n]$$

and its k-basis

$$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\}.$$

For each $\delta \in \mathbb{N}$ we will also set $\mathcal{T}_\delta := \{t \in \mathcal{T} : \deg(t) = \delta\}$.

2. We also fix an integer value $r \leq n$, set $d := n - r$ and consider

the field $K := k(V_1, \ldots, V_d)$,
its algebraic closure K and its universal field $\Omega(K) = \Omega(k)$,
the polynomial ring $\mathcal{Q} := K[Z_1, \ldots, Z_r]$ and
its K-basis $\mathcal{W} := \{Z_1^{a_1} \cdots Z_r^{a_r} : (a_1, \ldots, a_r) \in \mathbb{N}^r\}$.

All the notation introduced in the previous volumes will be applied also in this setting, with the proviso that everywhere $n, k, \mathcal{P}, \mathcal{T}$ are substituted by, respectively $r, K, \mathcal{Q}, \mathcal{W}$.

3. Each polynomial $f \in k[X_1, \ldots, X_n]$ is a unique linear combination,

$$f = \sum_{t \in \mathcal{T}} c(f, t)t,$$

of the terms $t \in \mathcal{T}$ with coefficients $c(f, t)$ in k and can be uniquely decomposed as $f = \sum_{\delta=0}^{d} f_\delta$, by setting

$$f_\delta := \sum_{t \in \mathcal{T}_\delta} c(f, t)t \quad \text{for each } \delta \in \mathbb{N},$$

where each f_δ is homogeneous, $\deg(f_\delta) = \delta$ and $f_d \neq 0$, so that $d = \deg(f)$.

4. Since, for each i, $1 \le i \le n$,

$$\mathcal{P} = k[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n][X_i],$$

each polynomial $f \in \mathcal{P}$ can be uniquely expressed as

$$f = \sum_{j=0}^{D} h_j(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)X_i^j \quad h_D \neq 0,$$

and

$$\deg_{X_i}(f) := \deg_i(f) := D$$

denotes its degree in the variable X_i.

In particular, for $i = n$, we have

$$f = \sum_{j=0}^{D} h_j(X_1, \ldots, X_{n-1})X_n^j, \quad h_D \neq 0, \quad D = \deg_n(f);$$

the *leading polynomial* of f is $\mathrm{Lp}(f) := h_D$, and its *trailing polynomial* is $\mathrm{Tp}(f) := h_0$.

5. Given a finite basis $F := \{f_1, \ldots, f_u\} \subset \mathcal{P}$, we denote as

$$\mathbb{I}(F) := (F) := \left\{\sum_{i=1}^{u} h_i f_i : h_i \in \mathcal{P}\right\} \subset \mathcal{P}$$

the ideal generated by F, and as

$$\mathcal{Z}(F) := \{\mathsf{a} \in \mathsf{k}^n : f(\mathsf{a}) = 0, \text{ for all } f \in F\} \subset \mathsf{k}^n$$

the algebraic variety consisting of each common root of all polynomials in F.

6. The support

$$\mathrm{supp}(f) := \{t \in \mathcal{T} : c(f, t) \neq 0\}$$

of f being finite, once a term ordering[1] $<$ on $\mathcal{T}$ is fixed, f has a unique representation as an ordered linear combination of terms:

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in k \setminus \{0\}, \quad t_i \in \mathcal{T}, \quad t_1 > \cdots > t_s.$$

The *maximal term* of f is $\mathbf{T}(f) := t_1$, its *leading cofficient* is $\mathrm{lc}(f) := c(f, t_1)$ and its *maximal monomial* is $\mathbf{M}(f) := c(f, t_1)t_1$.

7. For any set $F \subset \mathcal{P}$ we write

- $\mathbf{T}_<\{F\} := \{\mathbf{T}(f) : f \in F\}$,
- $\mathbf{T}_<(F) := \{\tau\mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$,

[1] A well-ordering $<$ on $\mathcal{T}$ will be called a term ordering if it is a semigroup ordering.

- $\mathbf{N}_<(F) := \mathcal{T} \setminus \mathbf{T}_<(F)$,
- $k[\mathbf{N}_<(F)] := \mathrm{Span}_k(\mathbf{N}_<(F))$

and we will usually omit the dependence on $<$ if there is no ambiguity.

8. Let $<$ be a term ordering on $\mathcal{T}$, $\mathsf{I} \subset \mathcal{P}$ an ideal and $\mathsf{A} := \mathcal{P}/\mathsf{I}$.
Since $\mathsf{A} \cong k[\mathbf{N}_<(\mathsf{I})]$, there is, for each $f \in \mathcal{P}$, a unique

$$g := \mathrm{Can}(f, \mathsf{I}, <) = \sum_{t \in \mathbf{N}_<(\mathsf{I})} \gamma(f, t, <)t,$$

the *canonical form*, such that

$$g \in k[\mathbf{N}(\mathsf{I})] \quad \text{and} \quad f - g \in \mathsf{I}.$$

9. For an ideal $\mathsf{I} \subset \mathcal{P}$,

$$\mathsf{I} := \cap_{i=1}^{\mathsf{t}} \mathfrak{q}_i$$

denotes an irredundant primary representation in $\mathcal{P}$; $d := \dim(\mathsf{I})$ its dimension and $r := r(\mathsf{I}) := n - d$ its rank; for each i, $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ is the associated prime.

10. For such an ideal I we will re-enumerate and re-label the variables as follows:

$$\{X_1, \ldots, X_n\} = \{V_1, \ldots, V_d, Z_1, \ldots, Z_r\},$$

so that

$$\mathsf{I} \cap k[V_1, \ldots, V_d] = (0), \quad d := \dim(\mathsf{I}),$$

and we will wlog assume that the primaries are ordered so that, for a suitable value $1 \leq \mathsf{r} \leq \mathsf{t}$,

$$\mathfrak{q}_i \cap k[V_1, \ldots, V_d] = (0), \quad \dim(\mathfrak{q}_i) = d \iff i \leq \mathsf{r}$$

so that the ideal

$$\mathsf{J} := \mathsf{I}k(V_1, \ldots, V_d)[Z_1, \ldots, Z_r] = \mathsf{I}\mathcal{Q}$$

is zero-dimensional and has, in $\mathcal{Q}$, the irredundant primary representation

$$\mathsf{J} := \cap_{i=1}^{\mathsf{r}} \mathfrak{q}_i \mathcal{Q}.$$

11. In general, when dealing with a zero-dimensional ideal, instead of

$$\mathsf{I} \subset \mathcal{P} = k[\mathcal{T}] = k[X_1, \ldots, X_n]$$

we prefer to use the notation

$$\mathsf{J} \subset \mathcal{Q} = K[\mathcal{W}] = K[Z_1, \ldots, Z_r].$$

12. For such a zero-dimensional ideal J, with a slight abuse of notation we will still set $\mathsf{A} := \mathcal{Q}/\mathsf{J}$ and denote as q_i its primary components in $\mathcal{Q}$; we also assume that

$$s := \deg(\mathsf{J}) = \dim(\mathsf{A})$$

and we denote, for each $f \in \mathcal{Q}$, $[f] \in \mathsf{A}$, its residue class modulo J and as Φ_f the endomorphism

$$\Phi_f : \mathsf{A} \to \mathsf{A}, \quad [g] \mapsto [fg].$$

13. In terms of a K-basis $\mathbf{q} = \{[q_1], \dots, [q_s]\}$ of A such that $\mathsf{A} = \mathrm{Span}_K(\mathbf{q})$, for each $g \in \mathcal{Q}$ the *Gröbner description of* g (Definition 29.3.3,) is the unique (row) vector

$$\mathbf{Rep}(g, \mathbf{q}) := (\gamma(g, q_1, \mathbf{q}), \dots, \gamma(g, q_s, \mathbf{q})) \in K^s,$$

which satisfies

$$[g] = \sum_j \gamma(g, q_j, \mathbf{q})[q_j].$$

14. A *Gröbner representation* (Definition 29.3.3) of J (or, better, of the algebra A) is the assignment of

- a K-linearly independent set $\mathbf{q} = \{[q_1], \dots, [q_s]\}$,
- the set $\mathcal{M} = \mathcal{M}(\mathbf{q}) := \left\{\left(a_{lj}^{(h)}\right) \in K^{s^2}, 1 \le h \le r\right\}$ of r square matrices,
- s^3 values $\gamma_{ij}^{(l)} \in K$,

which satisfy

(1) $\mathcal{Q}/\mathsf{J} \cong \mathrm{Span}_K(\mathbf{q})$,

(2) $[Z_h q_l] = \sum_j a_{lj}^{(h)}[q_j]$ for each $l, j, h, 1 \le l, j \le s, 1 \le h \le r$,

(3) $[q_i q_j] = \sum_l \gamma_{ij}^{(l)}[q_l]$ for each $l, j, h, 1 \le i, j, l \le s$.

A Gröbner representation is called a *linear representation* iff $\mathbf{q} = \mathbf{N}_<(\mathsf{J})$ w.r.t. a term ordering $<$.

15. For the zero-dimensional ideal $\mathsf{J} \subset \mathcal{Q}$ with irredundant primary representation $\mathsf{J} = \bigcap_{i=1}^{\mathsf{r}} \mathsf{q}_i$ in $\mathcal{Q}$, we set, for each i, $1 \le i \le \mathsf{r}$,

- $\mathfrak{m}_i = \sqrt{\mathsf{q}_i}$, the associated maximal prime,
- $K_i := \mathcal{Q}/\mathfrak{m}_i$, $K \subset K_i \subset \mathsf{K}$,
- $\mathcal{Q}_i := K_i[Z_1, \dots, Z_r]$,
- the irredundant primary representations $\mathsf{q}_i = \cap_{j=1}^{r_i} \mathsf{q}_{ij}$ and $\mathfrak{m}_i = \cap_{j=1}^{r_i} \mathsf{m}_{ij}$ in $\mathcal{Q}_i$,
- the roots $\mathsf{b}_{ij} := (b_1^{(ij)}, \dots, b_r^{(ij)}) \in K_i^r \subset \mathsf{K}^r$, $1 \le j \le r_i$,
- $d_{ij} := \mathrm{mult}(\mathsf{b}_{ij}, \mathsf{J}) = \deg(\mathsf{q}_{ij})$ for each j, $1 \le j \le r_i$,

which satisfy:

(1) $\mathsf{m}_{ij} = (Z_1 - b_1^{(ij)}, \dots, Z_r - b_r^{(ij)})$,

(2) the b_{ij}, $1 \le j \le r_i$, are K-conjugate for each i,

(3) up to a renumeration, $\sqrt{\mathsf{q}_{ij}} = \mathsf{m}_{ij}$,
(4) $\mathfrak{m}_i = \mathsf{m}_{ij} \cap \mathcal{Q}$,
(5) $\mathfrak{q}_i = \mathsf{q}_{ij} \cap \mathcal{Q}$,
(6) for each $j, l, 1 \le j, l \le r_i$, $d_{ij} = d_{il} =: d_i$,
(7) $r_i = \deg(\mathfrak{m}_i) = [K_i : K]$,
(8) $\deg(\mathfrak{q}_i) = d_i r_i$,
(9) $\mathsf{J} = \cap_{i=1}^{\mathsf{r}} \cap_{j=1}^{r_i} \mathsf{q}_{ij}$, $\sqrt{\mathsf{J}} = \cap_{i=1}^{\mathsf{r}} \cap_{j=1}^{r_i} \mathsf{m}_{ij}$, are the irredundant primary representations in $\mathsf{K}[Z_1, \dots, Z_r]$,
(10) $\mathcal{Z}(\mathsf{J}) = \{\mathsf{b}_{ij} : 1 \le i \le \mathsf{r}, 1 \le j \le r_j\}$,
(11) $\sum_{i=1}^{\mathsf{r}} d_i r_i = s$.

16. With the notation above the ideal J has $\mathsf{s} := \sum_{i=1}^{\mathsf{r}} r_i$ roots; we will also denote this set of roots as

$$\mathcal{Z}(\mathsf{J}) = \{\alpha_1, \dots, \alpha_{\mathsf{s}}\} \subset \mathsf{K}^r, \quad \alpha_i = (a_1^{(i)}, \dots, a_r^{(i)}).$$

For each such root α_i we write

- $\mathfrak{m}_{\alpha_i} = (Z_1 - a_1^{(i)}, \dots, Z_r - a_r^{(i)})$,
- $\mathfrak{q}_i$ as the $\mathfrak{m}_{\alpha_i}$-primary component of J, so that $\mathsf{J} = \cap_{i=1}^{\mathsf{s}} \mathfrak{q}_i$ in $\mathsf{K} \otimes_K \mathcal{Q}$,
- $s_i := \text{mult}(\alpha_i, \mathsf{J}) = \deg(\mathfrak{q}_i)$ as the multiplicity in J of α_i, so that $s = \sum_{i=1}^{\mathsf{s}} s_i$.

17. A linear form $Y := \sum_{h=1}^{r} c_h Z_h$ is said to be an *allgemeine coordinate* for the zero-dimensional ideal J (Definition 34.4.7) iff

(a) there are polynomials $g_i \in K[Y]$, $0 \le i \le n$, g_0 monic, $\deg(g_i) < \deg(g_0)$, such that

$$G := (g_0(Y), Z_1 - g_1(Y), Z_2 - g_2(Y), \dots, Z_r - g_r(Y))$$

is the reduced Gröbner basis of the ideal

$$\mathsf{J}^+ := \mathsf{J} + \left(Y - \sum_h c_h Z_h\right) \subset K[Y, Z_1, \dots, Z_r]$$

w.r.t. the lex ordering induced by $Y < Z_1 < \cdots < Z_r$;

with the present notation this condition implies, among other things, that (Corollary 34.4.6)

(b) $\mathcal{Q}/\mathsf{J} \cong K[Y]/g_0(Y)$
(c) for each i, $1 \le i \le \mathsf{s}$, $\beta_i := \sum_{h=1}^{r} c_h a_h^{(i)}$ is a root of g_0 with multiplicity s_i and
(d) $a_j^{(i)} = g_j(\beta_i)$ for each i, $1 \le i \le \mathsf{s}$, and each j, $1 \le j \le r$,
(e) $g_0(Y) = \prod_{i=1}^{r} (Y - \beta_i)^{s_i}$,
(f) $f \in \mathsf{J} \iff \mathbf{Rem}(f(g_1(Y), \dots, g_r(Y)), g_0(Y)) = 0$.

Moreover, there is a Zarisky open set $\mathbf{U} \subset K^n$ such that $Y := \sum_{h=1}^{r} c_h Z_h$ is an *allgemeine* coordinate for J iff $(c_1, \dots, c_r) \in \mathbf{U}$.